

42390P13736

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

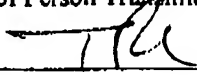
In re Application of: )  
 )  
Glew, et al ) Examiner: Pyzocha, Michael J.  
for Intel Corporation )  
 )  
Serial No.: 10/039,961 ) Art Unit: 2137  
 )  
Filing Date: December 31, 2001 )  
 )  
For: PROCESSOR SUPPORTING )  
EXECUTION OF AN )  
AUTHENTICATED CODE )  
INSTRUCTION )

**CERTIFICATE OF MAILING/TRANSMISSION**

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date indicated below and that this paper has been addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, fax number (571) 273-8300.

Date of Deposit: January 28, 2010

Name of Person Transmitting Correspondence:

  
\_\_\_\_\_  
Signature1/28/10  
\_\_\_\_\_  
Date

Mail Stop Appeal Brief Patents  
Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

**APPEAL BRIEF**

42390P13736

PATENT

TABLE OF CONTENTS

REAL PARTY IN INTEREST	3
RELATED APPEAL AND INTERFERENCES	4
STATUS OF CLAIMS	5
STATUS OF AMENDMENTS	6
SUMMARY OF CLAIMED SUBJECT MATTER	7
GROUND OF REJECTION TO BE REVIEWED ON APPEAL	8
ARGUMENT	9
CLAIMS APPENDIX	11
EVIDENCE APPENDIX	15
RELATED PROCEEDINGS APPENDIX	16

42390P13736

PATENT

REAL PARTY IN INTEREST

The real party in interest is the assignee Intel Corporation.

42390P13736

PATENT

RELATED APPEAL AND INTERFERENCES

None.

42390P13736

PATENT

STATUS OF CLAIMS

Claims 1-2 (Rejected).

Claim 3 (Canceled).

Claims 4-6 (Rejected).

Claim 7 (Canceled).

Claims 8-9 (Rejected).

Claims 10-11 (Withdrawn).

Claims 12-18 (Rejected).

Claims 19-21 (Withdrawn).

Claims 22-23 (Rejected).

Claim 24 (Canceled).

Claims 25-26 (Withdrawn).

Claims 27-29 (Canceled).

Claims 30-31 (Withdrawn).

Claims 32-39 (Canceled).

Claims 1-2, 4-6, 8-9, 12-18, and 22-23 are rejected and are the subject of this Appeal Brief.

42390P13736

PATENT

STATUS OF AMENDMENTS

All amendments have been entered.

42390P13736

PATENT

SUMMARY OF CLAIMED SUBJECT MATTER

In the following discussion, the independent claim is read on one of many possible embodiments without limiting the claim.

1. A processor comprising  
memory (Fig. 3, 360);  
decode logic (Fig. 3, 340) to receive a launch instruction; and  
one or more execution units (Fig. 3, 370) to execute the launch instruction by  
loading an authenticated code module into the memory, locking the memory, retrieving a  
key, authenticating the authenticated code module stored in the memory using the key,  
and initiate execution of the authenticated code module stored in the memory.

At this point, no issue has been raised that would suggest that the words in the claims have any meanings other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

42390P13736

PATENT

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

- A. Whether claim 1 is unpatentable over U.S. Patent No. 6,651,171 ("England") in view of U.S. Patent No. 6,704,872 ("Okada").



42390P13736

PATENT

ARGUMENT

A. Is claim 1 unpatentable over England in view of Okada?

It is respectfully argued that the combination of England and Okada is improper. The examiner argues that the motivation to apply Okada to England is to provide a processor with a function to prevent the illegal execution of a program, which is an object of Okada (see column 3, lines 34 to 38). This object, therefore, is allegedly fulfilled by the disclosure of Okada. Therefore, the authentication operation of Okada is to limit the right to use a specific software program to a single processor (i.e., to authenticate the processor). In contrast, England has an entirely different object, which is to hide the execution of curtailed code from the normal operation of a system (see column 3, lines 36-44), and the authentication operation of England is to authenticate programs (see column 3, lines 60-64). Combining Okada and England would do nothing to help Okada prevent the illegal execution of a program or to help England hide the execution of curtailed code from the normal operation of a system. Therefore, there is no motivation to combine Okada and England.

More specifically, the examiner argues that England describes loading an authenticated code module into memory and locking the memory. Locking the memory, according to England, is disabling all accesses to memory apart from those initiated by the processor executing authorized code (see column 11, lines 40-43). There would be no reason to do this in connection with preventing the illegal execution of a program by a processor. The program would be accessible for execution by the processor, legally or illegally. England is clearly not related to preventing the illegal execution of a program.

42390P13736

PATENT

Therefore, the combination of Okada and England is improper and withdrawal of the rejections based on their combination is respectfully requested.

\* \* \*

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue. Please charge any necessary fees, including extension fees, to our Deposit Account No. 50-0221.

Respectfully submitted,



Date: January 28, 2010

---

Thomas R. Lane  
Registration No. 42,781

42390P13736

PATENT

CLAIMS APPENDIX

The claims on appeal are:

1. A processor comprising

memory;

decode logic to receive a launch instruction; and

one or more execution units to execute the launch instruction by loading an authenticated code module into the memory, locking the memory, retrieving a key, authenticating the authenticated code module stored in the memory using the key, and initiate execution of the authenticated code module stored in the memory.

2. The processor of claim 1 further comprising a cache memory that provides the memory.

4. The processor of claim 2 wherein the execution units lock the cache memory to prevent replacement of lines of the authenticated code module stored in the cache memory.

5. The processor of claim 1 wherein the execution units lock the memory to prevent other processors from altering the authenticated code module stored in the memory.

42390P13736

PATENT

6. The processor of claim 1 wherein the decode logic is also to generate one or more opcodes for the launch instruction, wherein the execution units authenticate and execute the authenticated code module in response to executing the one or more opcodes.

8. The processor of claim 1, wherein the execution units retrieve the key specified by one or more operands of the launch instruction.

9. The processor of claim 1, wherein the execution units, in response to the launch instruction, retrieve the key from a chipset.

12. The processor of claim 1, wherein the execution units, in response to the launch instruction, decrypt at least a portion of the authentication module stored in the memory.

13. The processor of claim 1, wherein the execution units, in response to the launch instruction, decrypt at least a portion of the authentication module to obtain a digest value, and determine whether the authentication module is authentic based upon the digest value.

42390P13736

PATENT

14. The processor of claim 1, wherein the execution units, in response to the launch instruction, obtain a digest value for the authentication code module, generate a computed digest value from at least a portion of the authenticated code module, and determine that the authenticated code module is authentic in response to the digest value and the computed digest value having a predetermined relationship.

15. The processor of claim 1, wherein the execution units, in response to the launch instruction, RSA-decrypt a signature of the authentication code module to obtain a digest value from the signature, perform a SHA-1 hash on the authenticated code module to generate a computed digest value, and determine that the authenticated code module is authentic in response to the digest value and the computed digest value being equal.

16. The processor of claim 1, wherein the execution units initiate execution of the authenticated code module only if the authenticated code module is determined to be authentic.

17. The processor of claim 16, wherein the execution units generate an error code in response to determining that the authenticated code module is not authentic.

18. The processor of claim 17, wherein the execution units generate a trap in response to determining that the authenticated code module is not authentic.

42390P13736

PATENT

22. The processor of claim 1, wherein the execution units authenticate and initiate execution of the authenticated code module stored in the memory in response to executing microcode associated with the launch AC instruction.

23. The processor of claim 1, embodied in a machine readable medium.

42390P13736

PATENT

EVIDENCE APPENDIX

None.

42390P13736

PATENT

RELATED PROCEEDINGS APPENDIX

None.



Intel Corporation  
4040 Lafayette Center Drive  
Chantilly, VA 20151

ATTORNEY CONFIDENTIAL

Intel Legal Team

# Fax

Page 1 of 8

Urgent

Confidential

Date: January 28, 2010

To:  
Examiner: Yong Choe  
USPTO

Fax:  
(571) 273-8300

Art Unit:  
2185

From:  
Thomas R. Lane  
Intel Corporation

Fax:  
(703) 633-0915

M/S:  
CY-LF2

Subject: Application No.: 11/618,450

Filed:  
December 29, 2006

Inventors:  
Koufaty

Docket No.:  
42390P23415

A CONFIRMATION COPY OF THIS DOCUMENT:  
WILL NOT BE SENT

I hereby certify that the below listed correspondence is being facsimile transmitted to the USPTO to Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on 1/28/10.  
Thomas R. Lane Date: 1/28/10 TLR

Included in this transmission:  
Fax Cover Sheet (1 page)  
Response to Restriction Requirement (7 pages)

#### Important Notice

This information is intended to be for the use of the individual or entity named on this transmittal sheet. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents of this faxed information is prohibited. If you have received this facsimile in error, please notify the sender by telephone immediately so that arrangements can be made for the retrieval of the original document at no cost to you.

42390P23415

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of:

Koufaty et al  
for Intel Corporation

Examiner: Choe, Yong J.

Serial No.: 11/618,450

Art Unit: 2185

Filing Date: December 29, 2006

For: PARTITIONING MEMORY  
MAPPED DEVICE  
CONFIGURATION SPACE**CERTIFICATE OF MAILING/TRANSMISSION**

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office on the date indicated below and that this paper has been addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, fax number (571) 273-8300.

Date of Deposit: January 28, 2010

Name of Person Transmitting Correspondence:

Signature

Date

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450**RESPONSE TO RESTRICTION REQUIREMENT**

Dear Sir:

In response to the restriction requirement mailed on December 28, 2009, please enter the following amendments and election.

42390P23415

PATENT

**AMENDMENTS TO THE CLAIMS**

1. (Original) An apparatus comprising:
  - a first configuration address storage location to store a first pointer to a first memory region to which transactions to configure a first plurality of devices in a partitioned system are addressed;
  - an access map storage location to store one of an access map and a pointer to an access map; and
  - addressing logic to use the access map to determine whether a configuration transaction from a partition to a first device in the first plurality of devices is to be allowed.
2. (Original) The apparatus of claim 1, further comprising a second configuration address storage location to store to store a second pointer to a second memory region to which transactions to configure a second plurality of devices in the partitioned system are addressed.
3. (Original) The apparatus of claim 1, wherein the addressing logic includes partition identification logic to generate a partition identifier based on the address provided by the configuration transaction.
4. (Original) The apparatus of claim 3, wherein the addressing logic includes look-up logic to look-up an entry for the first device in the access map.

42390P23415

PATENT

5. (Original) The apparatus of claim 3, wherein the addressing logic includes look-up logic to look-up an entry for the first device in the access map, based on a device identifier provided by the configuration transaction.
6. (Original) The apparatus of claim 4, wherein the look-up logic is also to look-up a sub-entry for the partition in the entry, to determine whether the configuration transaction is to be allowed.
7. (Original) The apparatus of claim 4, wherein the look-up logic is also to look-up a sub-entry for the partition in the entry, and to determine whether the configuration transaction is to be allowed, based on the partition identifier provided by the partition identification logic.
8. (Withdrawn) A method comprising:
  - receiving a request from a processor to access the configuration space of a device in a partitioned system, the partitioned system including a plurality of partitions;
  - determining a partition identifier for the request; and
  - determining whether the device is assigned to the one partition, of the plurality of partitions, corresponding to the partition identifier using an access map.
9. (Withdrawn) The method of claim 8, wherein determining a partition identifier

42390P23415

PATENT

includes determining the partition identifier based on the address provided by the request.

10. (Withdrawn) The method of claim 9, wherein determining the partition identifier based on the address provided by the request includes determining to which of a plurality of memory mapped configuration spaces the address belongs.
11. (Withdrawn) The method of claim 8, wherein determining whether the device is assigned to the one partition of the plurality of partitions includes looking up an entry for the device in an access map.
12. (Withdrawn) The method of claim 11, wherein looking up the entry for the device includes using a device identifier from the request to find the entry.
13. (Withdrawn) The method of claim 12, wherein determining whether the device is assigned to the one partition of the plurality of partitions includes looking up a sub-entry in the entry, where the sub-entry indicates whether the device is assigned to the one partition.
14. (Withdrawn) The method of claim 13, wherein determining whether the device is assigned to the one partition of the plurality of partitions is based on the partition identifier.

42390P23415

PATENT

15. (Original) A system comprising:
- a first partition including:
    - a first device, and
    - a first portion of a memory to which transactions to configure the first device are addressed; and
  - a second partition including:
    - a second device, and
    - a second portion of the memory to which transactions to configure the second device are addressed;
  - a storage location to store one of an access map and a pointer to an access map;
  - and
  - addressing logic to determine whether a device configuration transaction from a processor is to be allowed, based on the access map.
16. (Original) The system of claim 15, wherein the addressing logic includes partition identification logic to generate a partition identifier based on the address provided by the device configuration transaction.
17. (Original) The system of claim 16, wherein the addressing logic includes look-up logic to look-up an entry for the device configuration transaction in the access map.
18. (Original) The system of claim 16, wherein the addressing logic includes look-up logic to look-up an entry for the device configuration transaction in the access map,

42390P23415

PATENT

based on a device identifier provided by the configuration transaction.

19. (Original) The system of claim 17, wherein the look-up logic is also to look-up a sub-entry for the partition in the entry, to determine whether the device configuration transaction is to be allowed.
20. (Original) The system of claim 17, wherein the look-up logic is also to look-up a sub-entry for the partition in the entry, and to determine whether the device configuration transaction is to be allowed, based on the partition identifier provided by the partition identification logic.

42390P23415

PATENT

**ELECTION**

In response to the restriction requirement, invention group I is elected. Claims 1-7 and 15-20 encompass the elected invention. Accordingly, claims 8-14 have been withdrawn. Please charge any necessary fees, including extension fees, to our Deposit Account No. 50-0221.

Respectfully submitted,

Date: January 28, 2010



Thomas R. Lane  
Registration No. 42,781



Intel Corporation  
4040 Lafayette Center Drive  
Chantilly, VA 20151-1218

ATTORNEY CONFIDENTIAL

Intel Legal Team

**Fax**

Page 1 of 17

Urgent

Confidential

Date: January 28, 2010

To:  
Examiner: Michael Pyzocha  
USPTO

Fax:  
(571) 273-8300

Art Unit:  
2437

From:  
Thomas R. Lane  
Intel Corporation

Fax:  
(703) 633-0915

M/S:  
CY-LF2

Subject: Application No.: 10/031,961

Filed:  
December 31, 2001

Inventors:  
Glew

Docket No.:  
42390P13736

A CONFIRMATION COPY OF THIS DOCUMENT:  
WILL NOT BE SENT

I hereby certify that the below listed correspondence is being facsimile transmitted to the USPTO to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on 1/28/10.  
Thomas R. Lane Date: 1/28/10                     

Included in this transmission:  
Fax Cover Sheet (1 page)  
Appeal Brief (16 pages)

**Important Notice**

This information is intended to be for the use of the individual or entity named on this transmittal sheet. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents of this faxed information is prohibited. If you have received this facsimile in error, please notify the sender by telephone immediately so that arrangements can be made for the retrieval of the original document at no cost to you.